As the Applicants previously argued (Response of August 15, 2005, spanning pages 6-7),

> In the present invention ... the term "specific character string" refers to a character string used in a document to be accessed, such that, if the document includes the specific character string, access to the document is limited to a permitted user or permitted users in accordance with the access level associated with the specific character string (see application figures 2 and 3, and related discussion).

Okuno Detects Tampering. Okuno discloses a system for detecting tampering with a block of text. For each block for which tampering is to be detected, the user marks that block with "<*code*>" (Fig. 7A, col. 6, lines 3-12, and col. 34, line 24). Each text block is and also marked with a respective identifier, called a "justification identification code" ("xxxxxx" in Fig. 7B, col. 6, lines 17-24).[1] Thus, the user has identified the desired text blocks, and each text block is also individually marked. This corresponds to step S22 in Fig. 2 (col. 6, lines 25-28; note that Okuno refers to the text block as a text "element").

The user also enters a password (col. 6, lines 29-32 and col. 34, line 25).

The justification identification code ("xxxxxx") is "generated" from the user's password and the text block content (col. 6, lines 33-35), as shown in step S33 of Fig. 2 (col. 6, lines 53-54 and col. 34, lines 26-28; note that the "justification identification code" generated here is the "first code" in claim 1). The justification identification code is generated from the password and the text block in such a way that it is unique. If the text block had been altered in any way, then the resulting justification identification code would have been different.

---

[1] It is not clear from this passage whether the user enters the justification identification code, but at col. 6, line 34, Okuno states that the justification identification code is "generated," apparently by the computer.

The justification identification code is stored (col. 34, lines 29-30, col. 3, line 32, and Fig. 3, step S32). Tampering can be detected by regenerating the justification identification code (note, the regenerated code is the "second code" in claim 1, col. 34, line 36) and comparing it to the earlier justification code for the same text block (i.e., the "first code" of col. 34, line 26). If the first and second justification identification codes are different, then the text block has been tampered with (col. 34, lines 39-44).

The Examiner is invited to especially note that Okuno's "password" 31 is not used to control access, it is used to generate the justification identification code.

Okuno Does Not Disclose Access Control. The Examiner asserts that Okuno discloses "access controlling information" but this is believed to be incorrect. As discussed above, Okuno does not limit access. Instead, Okuno *permits* access, but *detects* when a particular type of access (i.e., modification, access level "0" in the Applicants' Fig. 3) has occurred. With respect, the text and drawing cited by the Examiner (Fig. 1 and col. 5, lines 52-59) do not disclose access controlling information. There is no mention the words "access," "controlling," "control," or "information" in the applied portion of the reference, nor is there any explanation in the Office Action of how the cited text and drawing amounts to a disclosure of "access controlling information" when that is not explicitly disclosed.

Okuno Actively Teaches *Against* Access Control. Okuno's Background section states (col. 1, line 43), that "with the conventional example [i.e., the prior art], permission for writing in or reading a file is only given to the owner [and] justification [i.e., authentication] of the document can be assured by inhibiting unauthorized users from writing. Accordingly, ... there were the following associated problems: 1. ... the document cannot be dealt with collectively. 2. It is not possible to meet a requirement of recognizing when [an illegal] rewrite has occurred ... 3. When the rewrite ... is made, there is no indication of the alteration."

Okuno avoids the complexity and uncertainty of access control by *detecting* tampering by an unauthorized user; and this is the teaching of the reference.

Further Discussion of Access Controlling Information. Further to the discussion above, the Examiner asserts that access controlling information including a specific character string and identification data for specifying said access controlling information corresponds to what is disclosed in lines 17- 52 in col. 6 of Okuno. However, what is disclosed there by Okuno is a means to determine whether or not a document is "valid" by the use of justification identification code. As was explained above, the justification identification code is generated by encoding the password assigned to each document creator and a text element, and is appended immediately after a punctuation symbol upon registration of the text element. Then confirmation of whether or not the document is valid is performed in such a manner that the justification identification code appended immediately after the punctuation symbol is compared with the document creator and the text element at the time of confirming the validity of the document. thereby determining as to whether or not the text element is the same one as the one having been registered.

In other words, the Examiner seems to consider that the access controlling information, specific character string and identification data according to the present invention correspond to the justification identification code, text element and password of Okuno, respectively. With respect, the above Examiner's opinion is incorrect. The claimed access controlling information is composed of a specific character string and an identification data, such that the access controlling information defines limitation of the user access in terms of the document including the specific character string.

On the contrary, the justification identification code of Okuno is a code for identifying whether or not the text element is created by the document creator specified by the password but is not the one for controlling user access.

Further, the claimed access controlling information includes the identification data for specifying the access controlling information, whereas the password disclosed by Okuno serves to specify the document creator. Therefore, these are different from each other.

Numao, Also, Does Not Disclose That Feature. Numao was previously applied as the primary reference, but was changed to the secondary reference due to the Applicants' amendment to "a specific character string and identification data *for specifying said access controlling information*" in claim 1. Numao was withdrawn as the primary reference in response to this amendment, which was deemed substantive by the Advisory Action of August 30, 2005. The earlier withdrawal of Numao is seen to constitute an admission that Numao does not disclose this feature. Thus, Numao cannot overcome the deficiencies of Okuno as noted above, even if it were applied against claim 1 (it is not).

Storage Means. The Examiner asserts that the claimed "a second storage means for registering access controlling information including a specific character string and identification data for specifying said access controlling information" corresponds to element 30 in Fig. 1 and its corresponding description in lines 52-59 in col. 5 of Okuno.

Element 30 in Fig. 1 of Okuno stores information such as to password, text element name, text element, encoded character string, justification identification code, comparison code, determination result, and owner name: however, the password of Okuno is not for limiting user access but, rather, for specifying a document creator. None of this information corresponds to the Applicants' claimed access controlling information. Thus, element 30 in Fig. 1 does not correspond to the claimed second storage means.

Adding Identification Data to the Document. The Examiner further asserts that "wherein said identification data is added to said document if said document includes said specific character string" according to the present claims corresponds to what is disclosed in lines 30-33, col. 6 of Okuno.

However, col. 6, lines 30-33 of Okuno only discloses that the document creator inputs the password, using a console to store it in a memory. The claimed invention appends the identification data to the document, and the identification data specifying the access control information corresponding to a specific character string if it is included in the document. But Okuno is silent on this function.

Access. The Examiner still further asserts that the claimed feature "access to said document is limited in accordance with contents of said access controlling information, when the access to said document is thereafter requested, if said document contains said added identification data" corresponds to what is disclosed in line 44, col. 7 to line 28, col. 8, and the Abstract, in Okuno. However, as stated above, lines 44, col. 7 to lines 28, col. 8 of Okuno discloses a processing step to determine whether or not the text element is valid, followed by displaying a determination result thereof. Therefore, it differs from the above-stated method to control access to the document described in claim 1. As was already noted above, Okuno discloses a mechanism making it possible to create and register text while allowing for the confirmation of the validity for each text element, and to confirm whether or not each text element is valid. Therefore, it differs from the claimed invention which provides a mechanism to control access to the document.

[5-6] Claims 2-16 are rejected under §103 over Okuno in view of Numao. This rejection is respectfully traversed.

Claim 2. The Examiner asserts that "It would have been obvious to one with ordinary skill in the art at the time the invention was made to apply the teaching of Numao into the invention of Okuno because the combination would increase the security of the document by limiting access to document using the identification data and the specific character string."

However, as stated above, Okuno fails to teach features corresponding to the claimed identification data and the specific character string, respectively.

Claims 3 and 16. The Examiner asserts that "wherein it is defined whether or not said document includes said specific character string at one of a time when said document is registered ... and a time when the access to said document is requested" according to the present claims corresponds to element 401 in Fig. 4 and lines 61-65 in col. 9 of Numao, and that a combination of Okuno and Numao discloses the claimed invention.

With respect, 401 in Fig. 4 of Numao is not a step for defining whether or not said document includes the specific character string but, rather, a step for searching a policy description corresponding to an access request.

Numao discloses in lines 61-65 of col. 9 that upon receiving the access request 110 or 130, the policy evaluation module 10 detects, from the resource document 40, a policy description 140 that corresponds to the document that is to be accessed (step 401), and performs an evaluation of the extracted policy description 140 (step 402). In contrast to the present claims, the policy description 140 of Numao is not so structured as to determine whether or not the specific character string is included in the document.

As stated above, neither Okuno nor Numao teaches the claimed feature, "it is defined whether or not said document includes said specific character string."

Claims 6-8, 10, and 13. With regard to the claimed feature "said controlling information is provided in a single record comprising a plurality of fields, including ID information for identifying said record, and ID information is added to the document for relating said access controlling information to the document," the Examiner summarizes, "See Fig. 6 of Numao, wherein the Access control policy rules are disclosed. The rule includes plurality of fields (subject, object, conditions). The ID information corresponds to the object name or the target document to be accessed."

However, the Applicants respectfully submit that ID information according to the present invention is for identifying the record, such that it corresponds neither to an object name nor the target document to be accessed.

The Applicants' previous arguments regarding Numao are reiterated by reference.[2]

Reconsideration and allowance are requested.

Respectfully submitted,

March 6, 2006
Date

Nick Bromer (Reg. No. 33,478)
(717) 426-1664
RABIN & BERDO, P.C.
CUSTOMER NO. 23995
Telephone: (202) 371-8976
Telefax : (202) 408-0924

I certify that this correspondence is being facsimile transmitted to the United States Patent and Trademark Office (fax no. 571-273-8300) on March 6, 2006.

Nick Bromer [reg. no. 33,478] *Signature*

[2] E.g., the Applicants previously argued, "The Examiner's arguments do not appear to address the limitation "wherein said identification data is added to said document if said document includes said specific character string," recited in claim 1. In Numao, access to documents in data file 210 (figure 2) is determined in access control subsystem 240 on the basis of a "policy description" 140 figure 3). As described in the Background Art section of Numao (see, for example, column 1, lines 17-27), the term "policy description" refers to one of a set of rules used to determine whether to permit access, the rules being arranged in a list of elements commonly called an access control list (ACL). In Numao, the ACL consists of a Subject (access permitted user), Object (target to be accessed), Operation (access permitted operation) and Condition (access permission condition) (see, for example, Figure 6 and description in col. 11, lines 35-42). Numao describes the policy descriptions 140 as residing in the resource document 40. Numao fails to teach or even suggest that a policy description, or any specific data included in a policy description, is added to a document to be accessed by a user, as claim 1 would require." The Applicants also argued for the dependent claims.